УДК 343.98
DOI https://doi.org/10.32689/2522-4603.2022.1.1

Василь БІЛОУС
кандидат юридичних наук, доцент кафедри криміналістики, доцент, Національний юридичний університет імені Ярослава Мудрого, вул. Пушкінська, 77, Харків, Україна, 61002, v.v.bilous@nlu.edu.ua
ORCID: 0000-0003-3535-7838

Катерина ЛАТИШ
кандидат юридичних наук, асистент кафедри криміналістики, Національний юридичний університет імені Ярослава Мудрого, вул. Пушкінська, 77, Харків, Україна, 61002, latysh78@gmail.com
ORCID: 0000-0002-9110-116X

Vasil BILOUS
PhD in Law, Associate Professor at the Department of Criminalistics, Associate Professor, Yaroslav Mudryi National Law University,77 Pushkinska street, Kharkiv, Ukraine, 61002, v.v.bilous@nlu.edu.ua
ORCID: 0000-0003-3535-7838

Kateryna LATYSH
PhD in Law, Assistant at the Department of Criminalistics, Yaroslav Mudryi National Law University, 77 Pushkinska street, Kharkiv, Ukraine, 61002, latysh78@gmail.com
ORCID: 0000-0002-9110-116X

СУДОВІ ЕКСПЕРТИЗИ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ ЯК ФОРМА ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПІД ЧАС РОЗСЛІДУВАННЯ КОРУПЦІЙНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

FORENSIC EXAMINATION OF RADIO ELECTRONIC DEVICES AS A FORM OF USING SPECIAL KNOWLEDGE DURING INVESTIGATION OF CORRUPTION CRIMINAL OFFENSES

Під час розслідування корупційних кримінальних правопорушень найбільш поширеними є проблеми роботи з електронними носіями, на яких можуть міститися сліди таких правопорушень. Крім того, цифрові дані, які можуть мати значення для кримінального провадження, містяться на серверах, що знаходяться закордоном, та побудовані за хмарними технологіями на віддалених хостингах або перебувають у розпорядженні телекомунікаційних компаній.

***Метою** даної статті є дослідження проблемних питань вилучення та направлення на експертизу електронних носіїв інформації, на яких можуть міститися електронні сліди вчинення корупційних кримінальних правопорушень, а також дослідження можливостей судових експертиз у сфері інформаційних технологій як форми використання спеціальних знань.*

***Методологічну основу** даної статті склали методи аналізу та синтезу, а також результати опитування слідчих та судових експертів з проблемних питань призначення судових експертиз у сфері інформаційних технологій.*

***Наукова новизна** цієї статті полягає у генеруванні нового наукового знання і прикладних рекомендацій при збереженні вагомих класичних доктрин щодо технологічного підходу до дослідження цифрових (електронних) доказів, особливостей їхнього вилучення з урахуванням принципів збереження їхньої цілісності та незмінюваності електронних слідів, які на них містяться, через призму призначення судових експертиз у сфері інформаційних технологій.*

***Висновки**. Висвітлено форми використання спеціальних знань при розслідуванні корупційних кримінальних правопорушень, особливості збору електронних доказів та запропоновано перелік типових питань, які можуть ставитися на вирішення експертові при проведенні судових експертиз у сфері інформаційних технологій.*

***Ключові слова:** цифрові (електронні) докази, електронні сліди, інформаційні технології, корупційні кримінальні правопорушення, судова експертиза, участь спеціаліста у слідчій (розшуковій) дії, спеціальні знання.*

During the investigation of corruption offenses, the most common are problems with electronic devices, which may contain electronic traces of such offenses. In addition, digital data that may be relevant as a evidence to criminal proceedings is stored on servers located abroad and built on cloud technologies on remote hosting or available to telecommunications companies.

The aim *of this article is to study the problematic issues of seizure and referral of electronic devices, which may contain electronic traces of corruption offenses, as well as the possibility of forensic examinations in the field of information technology as a form of special knowledge.*

The methodological basis *of this article were methods of analysis and synthesis, as well as the results of a survey of investigative and forensic experts on problematic issues of appointment of forensic examinations in the field of information technology.*

The scientific novelty *of this article is to generate new scientific knowledge and applied recommendations while preserving important classical doctrines on the technological approach to the study of digital (electronic) evidence, the peculiarities of their removal, taking into account the principles of preserving their integrity and immutability of electronic traces. appointment of forensic examinations in the field of information technology.*

Conclusions. *The forms of using special knowledge in the investigation of corruption offenses, the peculiarities of collecting electronic evidence and a list of typical issues that can be addressed to the expert in conducting forensic examinations in the field of information technology are proposed in this article.*

Key words: *digital (electronic) evidence, electronic evidence, information technology, corruption criminal offences, forensic examination, the participation of a specialist in the investigation (search) activity, special knowledge.*

Актуальність проблеми. В умовах стрімкого розвитку інформаційних та інформаційно-телекомунікаційних технологій, масового поширення комп'ютерної техніки і різноманітного радіообладнання (радіоелектронних засобів), як то смартфони, планшетні комп'ютери, мобільні телефони тощо, зазнають трансформації усі без виключень процеси і явища. Не залишається осторонь науково-технічного прогресу і злочинність. Особливо корупційна, де невід'ємними характеристиками особи злочинця є високий інтелектуальний рівень, організаторські здібності, доступ до різноманітних ресурсів, професійний та життєвий досвід тощо.

Зазначене забезпечує систематичне здійснення складної злочинної діяльності, коли безпосередньому вчиненню злочину передують ретельне планування й організація, а по його вчиненні чи паралельно з ним – приховування слідів і предметів злочинного посягання одноосібно або із залученням значної кількості співучасників. Сучасні ж інформаційно-телекомунікаційні засоби, системи і технології надають можливість підтримувати злочинну комунікацію між останніми та вчиняти кримінальні правопорушення дистанційно. Не тільки у реальному, але й у віртуальному, кіберпросторі. Навіть предметом неправомірної вигоди все частіше постають криптовалюти, обіг яких відбувається у дискретній формі.

Аналіз останніх досліджень і публікацій. Широке коло проблемних питань використання спеціальних знань, їх види та форми у кримінальному судочинстві з давна досліджувалися у наукових працях таких вчених, як: Л. Ю. Ароцкер, В. П. Бахін, А. І. Вінберг, Г. Л. Грановський, В. Г. Гончаренко, В. А. Журавель, Н. І. Клименко, В. Я. Колдін, О. Н. Колесниченко, В. П. Колмаков, В. О. Коновалова, В. С. Кузьмічов, В. О. Образцов, М. В. Салтевський, М. Я. Сегай, М. О. Селіванов, В. Ю. Шепітько, О. М. Шрамко та ін. Однак сучасний технологічний устрій спонукає до розвитку міждисциплінарних зв'язків криміналістики з широким спектром технічних наук і генерування нового наукового знання і прикладних рекомендацій при збереженні вагомих класичних доктрин. Зазначене зумовлює перегляд усталених підходів до методики розслідування злочинів корупційної спрямованості й тактики провадження окремих слідчих (розшукових) дій та негласних слідчих (розшукових) дій, напрямів і форм застосування спеціальних знань.

Метою цієї статті є дослідження проблемних питань вилучення та направлення на експертизу електронних носіїв інформації, на яких можуть міститися електронні сліди вчинення корупційних кримінальних правопорушень, а також дослідження можливостей судових експертиз у сфері інформаційних технологій як форми використання спеціальних знань.

Виклад основного матеріалу дослідження. Необхідною умовою успішного розслідування корупційних кримінальних правопорушень є використання суб'єктами розслідування спеціальних знань у сфері комп'ютерних технологій. До структури таких спеціальних знань, які застосовують спеціалісти та експерти у сфері комп'ютерних технологій, відносять базові знання: з інформатики, комп'ютерної, програмної та системної інженерії, автоматизації та комп'ютерно-інтегрованих технологій, безпеки інформаційних і телекомунікаційних систем, систем технічного захисту інформації, управління інформаційною безпекою тощо [6, С. 14], а також спеціальні знання в галузі електротехніки, електроніки, радіотехніки та зв'язку. Без застосування криміналістичних та судово-експертних знань розслідування в межах кримінального процесу стає мертвим та бездоказовим. Але із глобалізацією світових процесів, розвитком технологій, швидкості передачі інформації,

нагальною проблемою стало утворення злочинності поза межею однієї держави та вихід її на міжнародний рівень, що стало викликом у протидії такій злочинності та необхідності спрямування криміналістичних та судово-експертних знань на допомогу правозастосовній діяльності [13, с. 179].

На думку О. М. Шрамка, спеціальні знання у галузі комп'ютерних технологій, що використовуються під час розслідування корупційних кримінальних правопорушень, – це поєднання сукупності знань про способи та методи розслідування із знаннями застосування програмно-технічних засобів, з метою більш ефективного забезпечення збирання, дослідження, оцінки та використання доказової інформації у кримінальних провадженнях зазначеної категорії [11, с. 74].

У кримінальному провадженні збирання доказів в електронній формі є достатньо складним процесом, що зумовлено складністю об'єктів та тим, що кожна дія на цифровому пристрої залишає певні сліди, у тому числі огляд та копіювання, адже більшість програм автоматично формують звіти та мають реєстр виконаних дій (логи). У зв'язку з цим рекомендується залучати відповідного спеціаліста (фахівця), який є достатньо підготовленим у цій сфері, оскільки навіть незначна некваліфікована дія з доказами в електронній формі може спричинити незворотну втрату цінної інформації [1, с. 12] та зміни файлових систем комп'ютера, що може призвести до сумнівів в автентичності змісту. На цьому ж наголошує Шепітько В. Ю., який вказує, що складність сучасних комп'ютерних інформаційних систем, технологій обробки цифрових даних потребує застосування засобів і технологій правоохоронного призначення, які повинні забезпечити: унеможливлення запису будь-яких даних або здійснення інших змін на носієві, що підлягає дослідженню на наявність слідів злочинної діяльності; максимальну універсальність підключення різних типів апаратних комп'ютерних засобів периферійного устаткування; функціональну підтримку програмними засобами огляду комп'ютерних даних, визначення чи перевірки контрольних файлів, копіювання даних на фізичному рівні їх представлення і запису на іншому носієві [12, с. 22].

М. І. Хавронюк також вказує на значну складність вилучення комп'ютерної техніки та електронних носіїв інформації у зв'язку з чим зазначає, що слід вживати заходів відносно збереження виявлених джерел доказів. Він рекомендує детально фіксувати не лише факт вилучення конкретного об'єкта, а й детально описувати, фотографувати його місцезнаходження у взаємозв'язку з іншими виявленими на місці предметами. Хоча для проведення цих дій рекомендується залучення відповідного фахівця, але й сам слідчий має володіти мінімумом знань для розуміння роботи комп'ютера та збереження електронної інформації [3, с. 37].

Зауважимо, що комп'ютерні засоби і програмне забезпечення розвиваються настільки стрімко, що своєчасне та повне виявлення і надійне збереження електронних доказів не можуть базуватися на мінімальній обізнаності представника гуманітарної професії. Тому є надзвичайно важливим залучення спеціаліста, яким у кримінальному провадженні є особа, яка володіє спеціальними знаннями та навичками і може надавати консультації, пояснення, довідки та висновки під час досудового розслідування і судового розгляду з питань, що потребують відповідних спеціальних знань і навичок. Спеціаліст має право користуватися технічними засобами, приладами та спеціальним обладнанням і може бути залучений для надання безпосередньої технічної допомоги (включно, але не вичерпно фотографування, складення схем, планів, креслень, відбір зразків для проведення експертизи тощо) сторонами кримінального провадження під час досудового розслідування і судом під час судового розгляду, а також для надання висновків у передбачених випадках (ч. 1 і 2, п. 2 ч. 4 ст. 71 Кримінального процесуального кодексу (далі – КПК) України) [5].

Фахове виявлення та вилучення електронних доказів створює надійні підвалини для результативного залучення у подальшому експерта, яким у кримінальному провадженні є особа, що володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України «Про судову експертизу» на проведення експертизи і якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та дати висновок з питань, які виникають під час кримінального провадження і стосуються сфери її знань (ч. 1 ст. 69 КПК України) [5].

При розслідуванні корупційних кримінальних правопорушень найчастіше призначають криміналістичні експертизи, експертизи матеріалів, речовин і виробів, комп'ютерно-технічні, фоноскопічні, відео-фоноскопічні, різноманітні товарознавчі, будівельно-технічні та оцінно-будівельні експертизи, експертизи вартості нерухомого майна та майнових прав на це майно, оцінно-земельні,

судово-бухгалтерські, біологічні та інші експертизи. До криміналістичних експертиз, які найчастіше призначаються, можна віднести: судову техніко-криміналістичну експертизу документів та судово-почеркознавчу експертизу, об'єктами яких є різноманітні документи, оформлені у зв'язку з виконанням тих чи інших службових дій, а також рукописні тексти та підписи, виконані службовими особами [7, с. 141].

Встановлення з'єднань між мобільними терміналами зв'язку (смартфонами, мобільними телефонами), якими користуються особи, а також місцезнаходження цих терміналів у період часу готування та вчинення цього кримінального правопорушення можна забезпечити шляхом тимчасового доступу до документів оператора телекомунікацій. Співставлення інформації щодо останнього може забезпечити одержання даних про зустрічі між такими особами [3, с. 37]. Крім того, важливим завданням є встановлення даних геопозиції та координат базових станцій для визначення місцезнаходження особи в певний час та використання цих даних в якості підтвердження доказів у кримінальному провадженні.

Дослідження вищевказаної цифрової інформації відбувається під час проведення судових експертиз, до числа яких належить комп'ютерно-технічна експертиза (далі – КТЕ), достатньо новий і перспективний рід судових експертиз, а також експертиза телекомунікаційних систем і засобів (дослідження цифрових та аналогових приладів) [12, с. 22]. Як було зазначено вище, ці експертизи є одними з ключових у кримінальному провадженні. За допомогою таких експертиз, зокрема, можна встановити наявність чи відсутність факту спілкування між сторонами кримінального процесу, зміст криміналістично значущої інформації, яка міститься на цифрових носіях, серед яких, зокрема: перелік номерів журналу дзвінків, надісланих, одержаних та збережених повідомлень (SMS, MMS, електронна пошта), зміст телефонної книги, нотаток, звукових, графічних, відео та інших файлів, у тому числі й видалених у період часу, коли був вчинений злочин, що розслідується) [3, с. 400]. Так, основними завданнями експертизи комп'ютерної техніки і програмних продуктів, за спеціальністю 10.9 «Дослідження комп'ютерної техніки та програмних продуктів», є: пошук та аналіз інформації на цифрових носіях (персональних комп'ютерах, серверах, мобільних пристроях тощо); відновлення видалених даних, пошук прихованої інформації; встановлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; встановлення Інтернет-активності користувача, кола спілкування, історії використання засобів зв'язку; дослідження технічного стану, характеристик, конструктивних особливостей комп'ютерної техніки та мобільних засобів [11, с. 203].

Експертиза телекомунікаційних систем і засобів за спеціальністю 10.17 «Дослідження телекомунікаційних систем (обладнання) та засобів» належить до інженерно-технічних судових експертиз. Це дослідження телекомунікаційних систем, засобів, мереж, їх складових, цифрових та аналогових приладів з метою встановлення технічних параметрів та стану об'єкта, визначення функціонального призначення, а також інформації, що ними передається, приймається та обробляється. Так, об'єктами цієї експертизи часто є: Інтернет, IP вузли, веб-сторінки, приймачі радіосигналів, вузли комутації; первинні мережі зв'язку, наземні станції супутникового зв'язку, обставини (адресації в мережі Інтернет; передачі радіосигналів; використання доменних імен у мережі Інтернет тощо) [9, с. 30]. Основними завданнями експертизи телекомунікаційних систем та засобів є: визначення характеристик та параметрів телекомунікаційних систем та засобів; встановлення фактів та способів передачі (отримання) інформації в телекомунікаційних системах; встановлення фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій; визначення якості надання телекомунікаційних послуг на рівні їх споживання; встановлення конфігурації та робочого стану телекомунікаційних систем та засобів; встановлення типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем та засобів; дослідження алгоритмів обробки інформації та її захисту у сфері телекомунікацій [2].

Вищезазначені дослідження відбуваються за Методикою комплексних досліджень комп'ютерних та телекомунікаційних систем у справах, пов'язаних з виявленням фактів спотворення процесу обробки інформації та порушення правил маршрутизації в мережах електрозв'язку з використанням технології VoIP, яка була розроблена у 2013 р. Київським НДІСЕ Міністерства юстиції України та зареєстрована у 2016 р. [8]. З огляду на це, не є об'єктивним твердження окремих науковців про відсутність затверджених Міністерством юстиції відповідних методик дослідження телекомунікаційної експертизи [4, с. 193]. Хоча слід погодитися з тим, що рівень науково-методичного забезпечення підґрунтя для

проведення даного виду експертиз залишається не достатнім. Так, якщо Реєстр методик судових експертиз передбачає 14 методик проведення комп'ютерно-технічної експертизи, то стосовно дослідження телекомунікаційних систем та засобів розроблено лише одну. Це знову ж таки свідчить про її новизну та недостатню дослідженість [10]. Особливостями існуючих методик експертного дослідження комп'ютерної техніки, програмних продуктів і телекомунікаційних мереж є те, що вони вимагають постійного оновлення та удосконалення у зв'язку з постійною зміною форматів представлення даних, операційних та файлових систем, протоколів передачі даних, технічних засобів передачі інформації. Цілком зрозуміло, що розробка й удосконалення таких методик можлива лише з використанням сучасного обладнання, програмного забезпечення та спеціальних знань фахівців у галузі телекомунікаційних систем і ІТ-технологій [4, с. 193].

Об'єктами експертизи комп'ютерної техніки і програмних продуктів при розслідуванні корупційних кримінальних правопорушень є вилучені під час процесуальних дій: комп'ютерна техніка (персональні комп'ютери (настільні, портативні), мережеві апаратні засоби (сервери, робочі станції, активне обладнання); носії інформації (дискети, жорсткі диски, CD-диски, флеш-карти тощо); периферійні пристрої (принтери, сканери, звукові карти); програмні продукти; портативні системи (смартфони, планшети, мобільні телефони тощо); вбудовані системи на основі мікропроцесорних контролерів (відео-реєстратори, цифрові камери, бортові комп'ютери); комплектуючі зазначених компонентів (апаратні блоки, плати розширення, мікросхеми тощо); пристрої, що не є комп'ютерами в класичному розумінні (електронні касові апарати, гральні автомати, карт-рідери тощо) [11, с. 203].

Часто виникають питання, пов'язані із наданням експертам дозволу на внесення змін, у мобільний телефон та наявну у ньому інформацію, які можуть призвести до зміни статусу об'єкту. Оскільки будь-які дії на технічному носієві призведуть до зміни його пам'яті та втрати статусу цілісності: навіть, якщо пристрій буде увімкнено та одразу вимкнено. Як вже зазначалося вище, із сформованих автоматично окремими програмами звітів та реєстрів виконаних дій, роздруківок логів та протоколу діяльності можна буде отримати інформацію про такі дії, що у подальшому може бути використано для заперечення цих доказів. Тому має бути вирішено питання надання експерту дозволу на повне або часткове знищення об'єкту експертизи (смартфону, іншого технічного носія) або зміну його властивостей та, у випадку, якщо наданий на експертизу смартфон виявиться заблокованим, надання в розпорядження експерта паролю (захисного коду до нього (у разі якщо слідство володіє зазначеною інформацією) для проведення комп'ютерно-технічної експертизи.

З огляду на викладене, на вирішення комп'ютерно-технічної експертизи смартфонів (мобільних телефонів) доцільно ставити такий перелік питань:

1. Який заводський номер (IMEI) смартфону (мобільного телефону) з наявними картками мобільного зв'язку оператора?

2. Чи наявний у смартфоні (мобільному телефоні), наданому на експертизу, журнал дзвінків, текстові SMS-повідомлення та телефона книга? У разі наявності зробити з них копію або вказати назви абонентів та їх абонентські номери.

3. Чи наявні у наданому на експертизу смартфоні (мобільному телефоні) повідомлення, передані через програми-месенджери? У разі наявності зробити з них копію.

4. Чи наявні у наданому на експертизу смартфоні (мобільному телефоні) у наявному та видаленому стані текстові, графічні, аудіо-, відео- файли? У разі наявності зробити з них копію.

5. Чи містяться в пам'яті наданого на дослідження смартфону (мобільного телефону) вебісторії, повідомлення в мережі Інтернет, а також файли користувача? При наявності зазначеної інформації виготовити з них копію.

6. Чи містяться на наданому на дослідженні смартфоні (мобільному телефоні) електронна переписка за допомогою програмних додатків та інтернет-месенджерів «Viber», «Messenger», «Telegram»», «WhatsApp», «Signal», «Line», у тому числі видалена, за номером смартфону (мобільного телефону)? Якщо так, то виготовити з них копію. Також рекомендується вказати назву іншого додатку або номер телефону конкретного абонента, з яким відбувалася переписка.

7. Чи містяться на наданому на дослідження смартфоні (мобільному телефоні) в інстальованих веб-браузерах історія відвідування мережі Інтернет, збережені логіни та паролі? На які веб-сайти мережі Інтернет та коли здійснювалися вихід з наданого на дослідження смартфону (мобільного телефону)?

8. Чи містяться на телефоні облікові дані (логіни та паролі) користувача для доступу до Інтернет ресурсів?

9. Яка інформація (файли з зображеннями, аудіо та відео файли) міститься на змінній карті пам'яті, розташованій у наданому на дослідження смартфоні (мобільному телефоні)?

10. Чи міститься на наданих на дослідження об'єктах серед наявних та видалених файлів зображення «зазначити шукану категорію»? Якщо так, то скопіювати зазначену інформацію.

11. Якщо відомі абонентські номери, пошук яких є метою судової експертизи, то питання експертові можуть мати такий вигляд: 11.1. Чи є у телефонній книзі смартфону (мобільного телефону) з наявною карткою мобільного зв'язку оператора «…» абонентський номер (зазначити який саме)? 11.2. Чи є у телефонній книзі смартфону (мобільного телефону) з наявною карткою мобільного зв'язку оператора «…» вхідні та вихідні телефонні виклики, вхідні та вихідні SMS та MMS повідомлення з певною особою (зазначити її ідентифікаційні дані) за номером мобільного телефону? Якщо так, то їх дата, час та тривалість?

12. Надати, шляхом копіювання на окремий носій Інтернет-дані з телефонної книги надаого на дослідження смартфону (мобільного телефону), а саме, збережені номери, зміст SMS повідомлень, дані GPS зі збереженими координатами.

Доступ до інформації, що міститься в смартфонах (мобільних телефонах) можливо отримати за допомогою програмно-апаратного засобу для дослідження мобільних пристроїв Cellebrite UFED Touch2, доступ до якого мають також спеціалісти відомчих управлінь оперативно-технічних заходів. У таких випадках призначається комплексна комп'ютерно-технічна експертиза на предмет наявності інформації щодо вмісту телефонної книги, історії дзвінків та текстових повідомлень (SMS MMS) в мобільних телефонах. Комплексною є експертиза, що проводиться із застосуванням спеціальних знань різних галузей науки, техніки або інших спеціальних знань (різних напрямів у межах однієї галузі знань) для вирішення одного спільного (інтеграційного) завдання (питання). До проведення таких експертиз у разі потреби залучаються як експерти експертних установ, так і фахівці установ та служб (підрозділів) інших центральних органів виконавчої влади або інші фахівці, що не працюють у державних спеціалізованих експертних установах [2].

Щодо проблеми копіювання на окремий носій Інтернет-даних з телефонних книг смартфонів (мобільних телефонів), а саме даних про збережені номери в телефонах, зміст SMS повідомлень, дані GPS зі збереженими координатами, слід враховувати, що такі дані відповідно до п. 7 та п. 8 ч. 1 ст. 162 КПК України відносяться до охоронюваної законом таємниці і процесуальний порядок їх отримання визначений у главі 15 розділу II КПК України. Під час судового провадження такий порядок регулюється ч. 2 ст. 333 КПК України шляхом надання тимчасового доступу до речей і документів із врахуванням причин, через які доступ не був здійснений під час досудового розслідування.

Отже, у статті висвітлено форми використання спеціальних знань під час розслідування корупційних кримінальних правопорушень, визначено особливості збору електронних доказів та запропоновано перелік типових питань, які можуть ставитися на вирішення експертові під час проведення судових експертиз у сфері інформаційних технологій.

Література:

1. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін. ; за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

2. Інструкція про призначення та проведення судових експертиз та експертних досліджень: наказ МЮУ від 08 жовтня 1998 р. № 53/5 / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/z0705-98?find=1&text=комплексн#w1_1 (дата звернення: 26.05.2022).

3. Корупційні схеми: їх кримінально-правова кваліфікація і досудове розслідування / за ред. М.І. Хавронюка. Київ : Москаленко О. М., 2019. 464 с.

4. Коршенко В. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *Jurnalul juridic naţional: teorie şi practică*. 2017. №. 2 (24). С. 192–194.

5. Кримінальний процесуальний кодекс України / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/4651-17#n958 (дата звернення: 26.05.2022).

6. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : автореф. дис. … канд. юрид. наук : спец. 12.00.09. Харків, 2007. 19 с.

7. Пілюков Ю. О., Шрамко О. М. Судова експертиза, як форма використання спеціальних знань при розслідуванні корупційних злочинів. *Актуальні проблеми правознавства.* Тернопіль, 2018. Вип. 4. С. 139–143.

8. Реєстр методик проведення судових експертиз : веб-сайт. URL: https://rmpse.minjust.gov.ua/search (дата звернення: 26.05.2022).
9. Самойленко О.А. Виявлення та розслідування кіберзлочинів : навч.-метод. посіб. Одеса. 2020. 112 с.
10. Шапошнікова І. Основні аспекти вибору типу і проведення експертизи у справах про кіберзлочинність : веб-сайт. URL: https://yur-gazeta.com/publications/practice/inshe/osnovni-aspekti-viboru-tipu-i-provedennya-ekspertizi-u-spravah-pro-kiberzlochinnist.html (дата звернення: 26.05.2022).
11. Шрамко О. М. Використання спеціальних знань під час розслідування корупційних кримінальних правопорушень : дис. … доктора філософії. Київ, 2021. 272 с.
12. Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України.* 2021. № 8. С. 12–27.
13. Shepitko, V.Yu., & Shepitko, M.V. The role of forensic science and forensic examination in international cooperation in the investigation of crimes. *Journal of the National Academy of Legal Sciences of Ukraine.* 2021. № 28(1). С. 179–186.

References:

1. Hutsaliuk M.V., Havlovskyi V.D., Khakhanovskyi V.H. (2020). *Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnomu provadzhenni [The use of electronic (digital) evidence in criminal proceedings].* O. V. Korneyko (Ed.). Kyiv : Vyd-vo Nats. Akad. Vnutr. sprav [in Ukrainian].
2. Instruktsiia pro pryznachennia ta provedennia sudovykh ekspertyz ta ekspertnykh doslidzhen, zatverdzhena nakazom MIuU 08.10.1998 № 53/5 [Instructions on the appointment and conduct of forensic examinations and expert examinations, Ordered by the Ministry of Internal Affairs of October 8, 1998 № 53/5]. Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98?find=1&text=kompleksn#w1_1 [in Ukrainian].
3. Khavroniuk, M.I. (Eds.). (2019). *Koruptsiini skhemy: yikh kryminalno-pravova kvalifikatsiia i dosudove rozsliduvannia [Corruption schemes: their criminal qualification and pre-trial investigation]*. Kyiv : PE "Moskalenko O. M." [in Ukrainian].
4. Korshenko, V. (2017). Sudova telekomunikatsiina ekspertyza yak dzherelo dokaziv pid chas rozsliduvannia kiberzlochyniv [Forensic telecommunications expertise as a source of evidence in the investigation of cybercrimes]. *Jurnalul juridic naţional: teorie şi practică*, 2 (24), 192–194 [in Ukrainian].
5. Kryminalnyi protsesualnyi kodeks Ukrainy (n.d.) [Criminal Procedure Code of Ukraine]. URL: https://zakon.rada.gov.ua/laws/show/4651-17#n958 [in Ukrainian].
6. Pashniev, D. V. (2007). Vykorystannia spetsialnykh znan pry rozsliduvanni zlochyniv, vchynenykh iz zastosuvanniam kompiuternykh tekhnolohii [Use of specialized knowledge in the investigation of crimes committed applied of computer technology]. Etended abstract of candidate's thesis. Kharkiv : KhNUVS [in Ukrainian].
7. Piliukov Yu. O., & Shramko O. M. (2018) Sudova ekspertyza, yak forma vykorystannia spetsialnykh znan pry rozsliduvanni koruptsiinykh zlochyniv [Forensic examination as a form of using special knowledge in the investigation of corruption crimes]. *Aktualni problemy pravoznavstva – Actual problems of law,* 4, 139–143 [in Ukrainian].
8. Reiestr metodyk provedennia sudovykh ekspertyz (n.d.) [Register of methods of conducting forensic examinations]. URL: https://rmpse.minjust.gov.ua/search [in Ukrainian].
9. Samoilenko, O.A. (2020) *Vyiavlennia ta rozsliduvannia kiberzlochyniv [Detection and investigation of cybercrime].* Odesa. [in Ukrainian].
10. Shaposhnikova, I. (2017) Osnovni aspekty vyboru typu i provedennia ekspertyzy u spravakh pro kiberzlochynnist [The main aspects of choosing the type and examination in cases of cybercrime]. URL: https://yur-gazeta.com/publications/practice/inshe/osnovni-aspekti-viboru-tipu-i-provedennya-ekspertizi-u-spravah-pro-kiberzlochinnist.html [in Ukrainian].
11. Shramko, O. M. (2021). Vykorystannia spetsialnykh znan pid chas rozsliduvannia koruptsiinykh kryminalnykh pravoporushen [Use of special knowledge in the investigation of corruption offenses]. Doctor of philosophy thesis. Kyiv [in Ukrainian].
12. Shepitko V., & Shepitko M. (2021). Doktryna kryminalistyky ta sudovoi ekspertyzy: formuvannia, suchasnyi stan i rozvytok v Ukraini [Doctrine of criminalistics and forensic science: formation, current situation and development in Ukraine]. *Pravo Ukrainy – Law of Ukraine,* № 8, 12–27 [in Ukrainian].
13. Shepitko, V.Yu., & Shepitko, M.V. (2021). The role of forensic science and forensic examination in international cooperation in the investigation of crimes. *Journal of the National Academy of Legal Sciences of Ukraine*, 28(1), 179–186 [in English].